NEW ZEALAND LAW SOCIETY

NZLS EST 1869

PRACTICE BRIEFING:

PROTECTING CLIENTS' PERSONAL INFORMATION

INTRODUCTION

The storage of personal and sensitive information on clients is an integral part of the work of a lawyer.

Developments in technology mean lawyers must have robust and secure procedures to protect their clients' personal information. The Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 require lawyers to protect and hold in strict confidence all information concerning a client which is acquired in the course of the professional relationship.

This Practice Briefing aims to give Law Society members helpful guidance on best practices for storing personal information. It is not intended to be an industry standard, nor does it provide a defence to misconduct or improper professional practice.

OBLIGATIONS TO PROTECT PERSONAL INFORMATION

Protecting personal information and confidentiality is part of a lawyer's professional obligations under the Rules of Conduct and Client Care. Any law firm or lawyer in sole practice also has obligations as an agency under the Privacy Act 1993.

Rules of Conduct and Client Care

The Rules of Conduct and Client Care outline the fundamental obligations of lawyers. The Rules make clear that whatever legal services a lawyer provides, he or she must provide the client with information about the work to be done, who will do it, and the way the services will be provided. Lawyers must also protect clients' privacy and ensure appropriate confidentiality.

Chapter 7 of the Rules of Conduct and Client Care states the requirements of information disclosure:

> Subject to limited exceptions, a lawyer must promptly disclose to a client all information that the lawyer has or acquires that is relevant to the matter in respect of which the lawyer is engaged by the client.

Also relevant is Chapter 8, which states the confidential information requirements:

> A lawyer has a duty to protect and to hold in strict confidence all information concerning a client, the retainer, and the client's business and affairs acquired in the course of the professional relationship.

And Chapter 11, which states the requirements of professional dealings:

> A lawyer's practice must be administered in a manner that ensures that the duties to the court and existing prospective, and former clients are adhered to, and that the reputation of the legal profession is preserved.
>
> A lawyer must take all reasonable steps to prevent any person perpetrating a crime or fraud through the lawyer's practice.

This includes taking reasonable steps to ensure the security of and access to electronic systems and passwords.

Privacy Act 1993

The Privacy Act 1993 defines "agency" as:

> any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector;

The Act is therefore applicable to lawyers who practise on their own account and law firms.

Lawyers and Conveyencers Act overrides Privacy Act

In many respects lawyers' obligations under the Privacy Act are consistent with obligations of confidentiality provided in the Rules of Conduct and Client Care. However, the Lawyers and Conveyancers Act 2006 will 'trump' the Privacy Act 1993 if there are inconsistencies between the two acts (see s.7 Privacy Act).

Penalties

Lawyers who breach their clients' privacy through either deliberate or inadvertent disclosure of personal information could find they have breached their professional obligations under the Lawyers and Conveyancers Act 2006.

While the Privacy Act 1993 provides guidelines to agencies, the Privacy Commissioner's Office doesn't currently have the power to fine or issue compliance notices. In serious cases the commissioner may refer the matter to the director of proceedings to initiate action in the Human Rights Review Tribunal. The government has indicated it will strengthen the Privacy Commissioner's powers, including the ability to create new offences, increase fines and issue compliance notices.

Adhering to the principles for dealing with personal information set out in the Privacy Act will help lawyers to meet their professional obligations under the Lawyers and Conveyancers Act 2006, and future proof their

practice against changes to the Privacy Commissioner's powers.

WHAT IS PERSONAL INFORMATION?

Most of the information which lawyers store on clients, who are private individuals, would fit the Privacy Act definition of 'personal information':

> **personal information** means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995).

Assistant Privacy Commissioner Katrine Evans has provided more information about what constitutes personal information in the speech *Personal information in New Zealand: between a rock and a hard place?* She says: "Personal information is a key concept in data protection statutes, including our own. But deciding what is, and what is not, personal information can be one of the hardest legal calculations in everyday privacy practice."

www.privacy.org.nz/news-and-publications/speeches-and-presentations/personal-information-in-new-zealand-between-a-rock-and-a-hard-place-katrine-evans/

PERSONAL INFORMATION STORAGE GOOD PRACTICE

Appoint a privacy officer

Section 23 of the Privacy Act requires all agencies to have a privacy officer.

This person is responsible for finding out what to do, and for giving advice to other members of staff on privacy related issues.

The Privacy Commissioner's Office can provide training to the privacy officer (*www.privacy.org.nz/how-to-comply/privacy-officers/*) and give the officer information about the Act.

The privacy officer should audit its privacy protection processes and health annually.

Follow the information privacy principles laid out in the Privacy Act 1993

The Act outlines 12 information privacy principles.

They deal with:

- collection of personal information (principles 1-4);
- storage and security of personal information (principle 5);

- requests for access to and correction of personal information (principles 6 and 7, plus parts 4 and 5 of the Act);
- accuracy of personal information (principle 8);
- retention of personal information (principle 9);
- use and disclosure of personal information (principles 10 and 11); and
- using unique identifiers (principle 12).

More information on the principles, along with guidelines, can be found on the Privacy Commissioner's website here: *http://privacy.org.nz/news-and-publications/guidance-notes/information-privacy-principles/*

Guidelines to personal information (Principles 1 and 2)

- The purpose for its collection must be lawful;
- The purpose must be connected with a function or activity of the agency; and
- The collection must be necessary for that purpose.
- The agency must collect the information directly from the individual concerned.
- The agency must not disclose a person's personal information without consent.

Although, the Privacy Act provides that an agency can only collect information directly from the individual concerned, collection of personal information on a third party may be lawful and necessary in some instances in regard to a lawyer representing a client.

Access to information and disclosure

A fundamental right under the Privacy Act 1993 is a person's right to access their personal information held by an agency. There are limited grounds for withholding personal information (see s.29 Privacy Act 1993 and information Privacy Principle 2).

Most Relevant for lawyers is the recognition that legal professional privilege overrides any right to access (s.29 (1)(f)).

Any new overriding ethical obligation may also effect access and disclosure, for instance, r.7 Rules of Conduct and Client Care or reporting provisions in other legislation such as Financial Transaction Reporting Act 1996.

STORAGE AND SECURITY OF PERSONAL INFORMATION

Principle 5 provides that an agency that holds personal information shall ensure:

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Written storage and security policy

Lawyers' and law firms' existing procedures for maintaining client confidentiality should go a long way to ensure compliance with the storage and security principle in the Privacy Act.

However, a written personal information privacy policy and staff guidelines are helpful in ensuring best practice. They are also evidence that a lawyer has taken "all reasonable steps to prevent any person perpetrating a crime or fraud through the lawyer's practice" under section 11 of the *Rules of Conduct and Client Care*.

Staff need to be trained adequately in these processes, which need to be followed in all their work.

Policy suggestions on personal information security

Below are some suggestions (not intended to be a comprehensive list) on how law firms and lawyers in sole practice can protect client's personal information:

Policy statements should specify how a lawyer or law firm is taking safe guards to protect personal information.

Be clear on what personal information can be **stored on different devices**, for example, portable devices, work stations, servers and the cloud, bring-your-own-device.

All devices that store personal information should be password protected. Consider implementing and running a mobile device management suite.

Data should be graded depending on the privacy risk that it poses.

High-risk data should not be emailed. Documents should be saved in network drives and accessed from there. Accidental emailing of documents to the wrong people is possibly the most common data-breach scenario.

Portable devices should have extra security measures such as encryption, password locks, remote wipe ability and physical security.

Limit access to data so only authorised parties can see personal information, physically or through the cloud.

Shred all hard copy files that are either high risk or medium risk.

Internal emails should not be forwarded to external parties.

Meetings should generally not be held at staff member's desk in case personal information is present.

Desks should be cleared of work papers containing personal information.

Networks should have access limitations implemented on the network file repository for any personal information that an employee is not privy too.

Homes or parked cars should not be used to visibly store papers, computers or other electronic devices.

Personal information audits

Lawyers and law firms are advised to annually audit the personal information they store.

This prevents the storage of unnecessary/no longer needed personal information. It also gives lawyers the opportunity to re-evaluate data and ensure that high risk information is being stored correctly and is safe.

WHAT INFORMATION SHOULD LAWYERS RETAIN?

As a matter of practice, the ownership of and obligations relating to documents should be discussed on establishment of a retainer.

Guidance on what information to retain and the length of time a practice should retain information is outlined in this opinion piece: *https://www.lawsociety.org.nz/__data/assets/pdf_file/0003/2883/opinion-ownership-rention-of-records.pdf*

RESPONDING TO A PRIVACY BREACH

Lawyers and law firms should have a plan for how they will deal with a privacy breach.

In cases of serious privacy breaches it is recommended that lawyers and law firms contact the Office of the Privacy Commissioner. It is likely future changes to the Privacy Act 1993 will include a mandatory reporting to the Privacy Commissioner in the instance of a serious privacy breach.

Key steps to take in response to a breach

The Office of the Privacy Commissioner recommends four key steps in responding to a privacy breach.

- Breach containment and preliminary assessment;
- Evaluation of the risks associated with the breach;
- Notification;
- Prevention.

A lawyer may also have overriding ethical obligations, in terms of both disclosure and communication of information to clients and the relationship of trust and confidence, to ensure clients are fully advised as to any potential compromise to privacy and confidentiality.

More information on containing a privacy breach can be found in the Data Safety Tool kit on the Office of the Privacy Commissioner's website, here: *http://privacy.org.nz/how-to-comply/data-safety-toolkit-preventing-and-dealing-with-data-breaches/*

Updated June 2014

New Zealand Law Society
Law Society Building
26 Waring Taylor Street
Wellington 6011

PO Box 5041
Lambton Quay
Wellington 6145

04 472 7837